

ABSTRACT

Networked computing entities which are members of a trusted group share knowledge of a secret value K that is unknown outside the trusted group. When an entity within the trusted group establishes a secure connection, it encodes its name along with the secret value K and an optional random number into a connection identifier. Encoding may use a hash function and/or encryption. By using this connection identifier and the secret value K, other members of the trusted group can decode the connection identifier and gain access to the specific secure connection by using the original cryptographic information for the connection. The connection identifier can be freely transmitted, with little risk that non-trusted entities will be able to use it to gain access to the secure connection.

/pc0